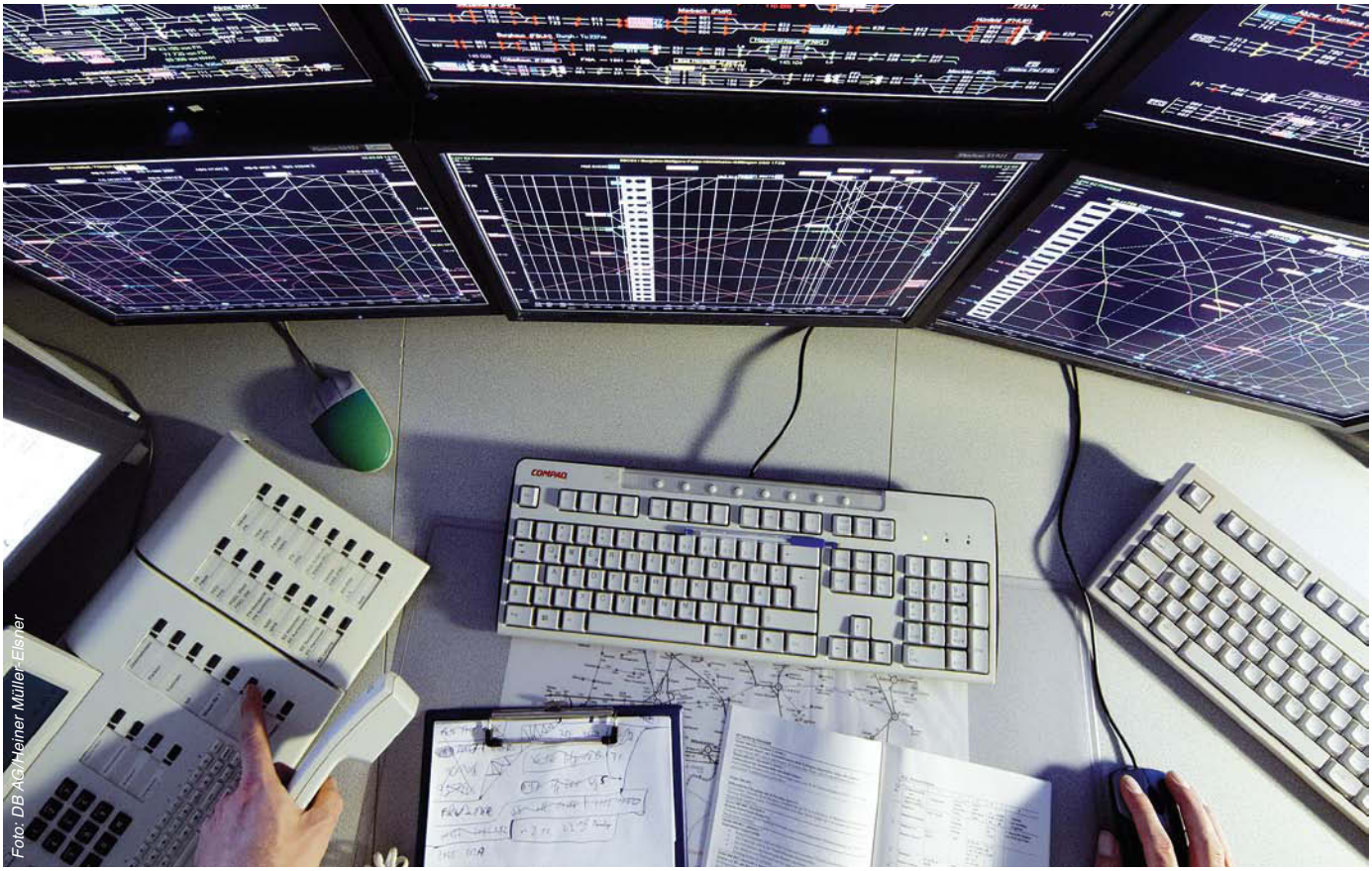


Foto: DB AG/Heiner Müller-Elsner

Common Safety Methods – Teil 3

Grundbegriffe für Sicherheits- und Risikobetrachtungen

Dr.-Ing. Gunnar Bosse, Institut für Eisenbahnwesen und Verkehrssicherung der Technischen Universität Braunschweig

In den beiden ersten Teilen dieser Beitragsreihe (Deine Bahn 12/2013, S. 18 ff. und 3/2014, S. 49 ff.) wurden die für Sicherheits- und Risikobetrachtungen elementaren Begriffe eingeführt, erläutert und gegeneinander abgegrenzt. In diesem dritten Teil werden mit der „Systemdefinition“ und der „Gefährdungsidentifikation“ zwei wesentliche Arbeitsschritte vorgestellt, die der Betreiber einer Eisenbahn, sei es als Infrastruktur- oder als Verkehrsunternehmer, durchzuführen hat, wenn er neue Systeme einführen oder an bestehenden Systemen entsprechend der CSM-Verordnung „signifikante“ Änderungen vornehmen möchte. Ferner werden die drei Risikoakzeptanzprinzipien erläutert, mit denen sichergestellt werden soll, dass neue oder veränderte Systeme einem allgemein akzeptierten Sicherheitsniveau entsprechen.

https://doi.org/10.24355/dbbs.084-202005050944-0

Unabhängig davon, ob ein vollkommen neues System eingeführt oder an einem bestehenden System „nur“ Veränderungen vorgenommen werden sollen, gehört die Systemdefinition zu den wesentlichen Aufgaben der für den Nachweis der Zulässigkeit erforderlichen Sicherheits- und Risikobetrachtungen. Von der Sorgfalt und der Qualität, mit der diese durchgeführt werden, hängt die Güte und Aussagekraft aller weiteren Prozessschritte ab. Deshalb sollen im Folgenden zunächst die Einordnung der Systemdefinition und ihre Bedeutung für die Sicherheits- und Risikoprozesse betrachtet werden. Anschließend wird auf ihre möglichen Inhalte eingegangen.

Systemdefinition

Einordnung in die Sicherheits- und Risikoprozesse

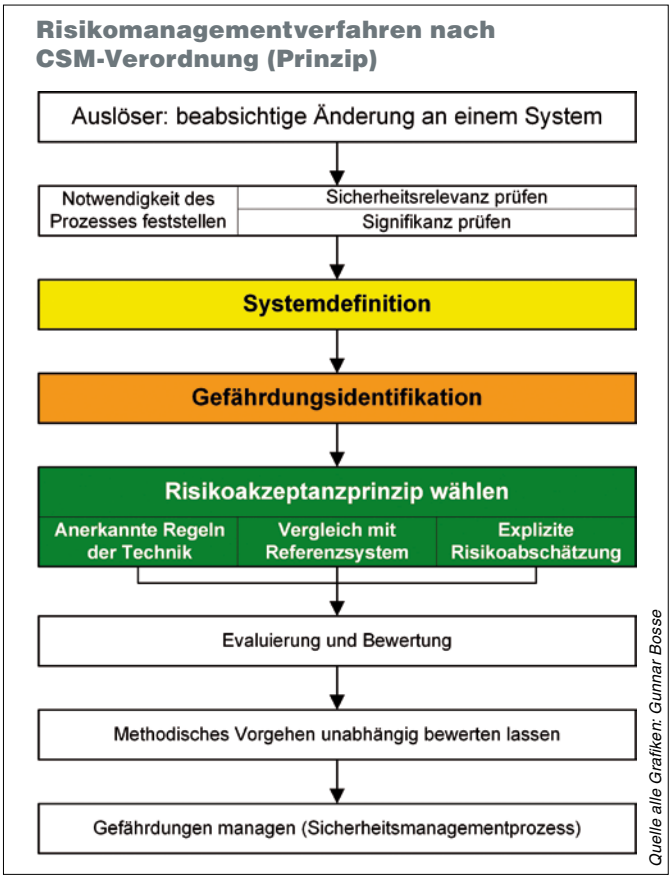
Die Systemdefinition gehört zu den ersten Prozessschritten, die im Rahmen von Sicherheits- und Risikobetrachtungen durchzuführen sind. In der Abbildung rechts wird der prinzipielle Ablauf solcher Sicherheitsbetrachtungen wiedergegeben, wie er beispielsweise im Falle einer Änderung an einem System gemäß CSM-Verordnung durchzuführen ist.

Bei genauer Betrachtung wird ein System gedanklich bereits definiert, wenn darüber nachgedacht wird, an ihm eine Änderung vorzunehmen. Dieser Schritt wird zwar noch nicht als Systemdefinition bezeichnet, doch kann eine Änderung nur beschrieben werden, wenn dargestellt wird, woran diese Änderung vorgenommen werden soll. In manchen Darstellungen wird deshalb in diesem Zusammenhang von einer „vorläufigen“ Systemdefinition“ gesprochen. Sie erlaubt bereits Entscheidungen, ob und in welchem Maß eine beabsichtigte Änderung sicherheitsrelevant ist. Die eigentliche und sehr viel detailliertere Systemdefinition wird nur durchgeführt, wenn auf Grund einer festgestellten Sicherheitsrelevanz Sicherheitsanalyseprozesse zu durchlaufen sind. Sie ist die Grundlage für die Identifizierung von Gefährdungen und die anschließende Bewertung der mit ihnen verbundenen Risiken.

Inhalte

Am Ende des zweitens Beitrags dieser Reihe wurde die Ebene der Gefährdungen als die wesentliche Schnittstelle zwischen der Betreiber- und Herstellerverantwortung hervorgehoben. Auf dieser Ebene werden seitens des Betreibers die Sicherheitsanforderungen in Form von Gefährdungsraten vorgegeben und seitens des Herstellers die Nachweise geführt, wie die Gefährdungen beherrscht und somit die vorgegebenen Anforderungen eingehalten werden. Gefährdungen, die seitens eines Betreibers übersehen und einem Hersteller weder qualitativ noch quantitativ als Anforderungen vorgegeben werden, können zu unerkannten Sicherheitslücken führen. Die Gefährdungen müssen deshalb möglichst vollständig identifiziert und dokumentiert werden. Eine ausreichend genaue und vollständige Systemdefinition ist dafür unabdingbar.

Es gibt kein Patentrezept oder strikte Vorgabe, wie eine Systemdefinition zu erstellen ist, da die zu betrachtenden Systeme auch innerhalb des Systems Eisenbahn sehr unterschiedlich sein können. Es bestehen daher gewisse Freiheitsgrade, eine Systemdefinition zu erstellen und auch ihren Umfang festzulegen.



Einordnung der Systemdefinition in ein formelles Risikomanagementverfahren

Doch es gibt Orientierungshilfen: Für den Bereich der Eisenbahnen empfiehlt die European Railway Agency (ERA) in der von ihr herausgegebenen Recommendation on the 1st set of Common Safety Methods, welche Punkte eine Systemdefinition umfassen sollte. Diese werden auch in die CSM-Verordnung als Anhaltspunkte vorgegeben.

Zu den wesentlichen Inhalten einer Systemdefinition gehören die Beschreibung der Systemfunktionen, ggf. das Benennen von Systemelementen und vorhandenen Sicherheitsvorkehrungen, das Ziehen von Systemgrenzen und die Beschreibung der mit dem System in Beziehung stehenden Nachbarsysteme einschließlich der Definition der physikalischen und funktionalen Schnittstellen. Hinzu kommen Angaben zu den Einsatzbedingungen des Systems sowie Annahmen, mit denen der Betrachtungsumfang des Risikobewertungsprozesses abgesteckt wird.

Die folgenden Erläuterungen und Hinweise sollen die möglichen Inhalte einer Systemdefinition begründen und veranschaulichen.

Systemfunktionen

Eine wichtige Grundlage für die Vollständigkeit von Gefährdungslisten ist das Definieren der Funktionen, die das betrachtete System betrieblich erbringen soll. Aus ihnen können die Betreiber, die Gefährdungen systematisch ableiten. Das Beschreiben der Systemfunktionen ist deshalb ein wesentlicher Bestandteil einer Systemdefinition. Eine gute Unterstützung kann zum Beispiel auch das Hinzuziehen oder die Bezugnahme zu bereits bekannten oder sogar vorhandenen Systemelementen sein.

https://doi.org/10.24355/dbbs.084-202005050944-0

Diese können menschlicher, technischer und betrieblicher Natur sein. Gerade bei bereits vorhandenen Systemen, an denen Änderungen vorgenommen werden sollen, kann es beim Erstellen eines Systemdefinition sehr hilfreich sein, sich beim Definieren der Systemfunktionen an den „Aufgaben" dieser Systemelemente zu orientieren. Deren „Aufgaben" sind letztlich nichts anderes als die gesuchten Systemdefinitionen.

Nachbarsysteme und Systemgrenzen

Es liegt auf der Hand, dass die Beschreibung eines zu betrachtenden Systems nicht ausufern darf. Der Arbeitsumfang sollte möglichst auf das erforderliche Maß begrenzt und die gesamte Analyse handhabbar, überschaubar und nachvollziehbar gehalten werden.

Deshalb wird man in Sicherheits- und Risikobetrachtungen, die beispielsweise einer Gleisfreimeldetechnologie gelten sollen, nicht das Gesamtsystem Eisenbahn betrachten und beschreiben, sondern bestrebt sein, ein Teilsystem Gleisfreimeldung als das zu betrachtende System einzugrenzen und es gegenüber Nachbarsystemen, wie zum Beispiel Fahrzeugen oder Stellwerksinnenlagen, abzugrenzen. Eine Systemdefinition hat somit auch die Aufgabe, das System gegenüber seinen Nachbarsystemen abzugrenzen und die Systemgrenzen festzulegen. In der praktischen Durchführung ist es oft hilfreich, nicht nur aufzuschreiben, was als zum System dazugehörig gelten soll, sondern auch, was nicht mit einbezogen werden soll.

Schnittstellen zu den Nachbarsystemen

Das Abgrenzen von Nachbarsystemen bedeutet nicht, dass diese vollkommen ausgeblendet werden dürfen, denn alle Teilsysteme eines Gesamtsystems stehen miteinander in Verbindung, sei es physikalisch oder mechanisch, wie zum Beispiel zwischen den Teilsystemen Fahrzeug und Fahrweg, oder in Form eines Datenaustausches, wie beispielsweise zwischen einer Gleisfreimeldeeinrichtung und einer Stellwerksinnenanlage, deren Ein- und Ausgabeschnittstellen ebenfalls zu beschreiben sind. Die Schnittstellenbeschreibungen müssen gegebenenfalls auch bestimmte Eigenschaften eines Nachbarsystems umfassen. Zum Beispiel kann es für das Funktionieren einer zu entwickelnden Gleisfreimeldeeinrichtung von Bedeutung sein, ob zwischen den Rädern einer Fahrzeugachse eine elektrische Verbindung besteht oder nicht. Es ist deshalb unerlässlich, im Rahmen einer Systemdefinition an den Systemgrenzen auch die Schnittstellen zu den benachbarten Systemen zu beschreiben.

Betriebliche Randbedingungen

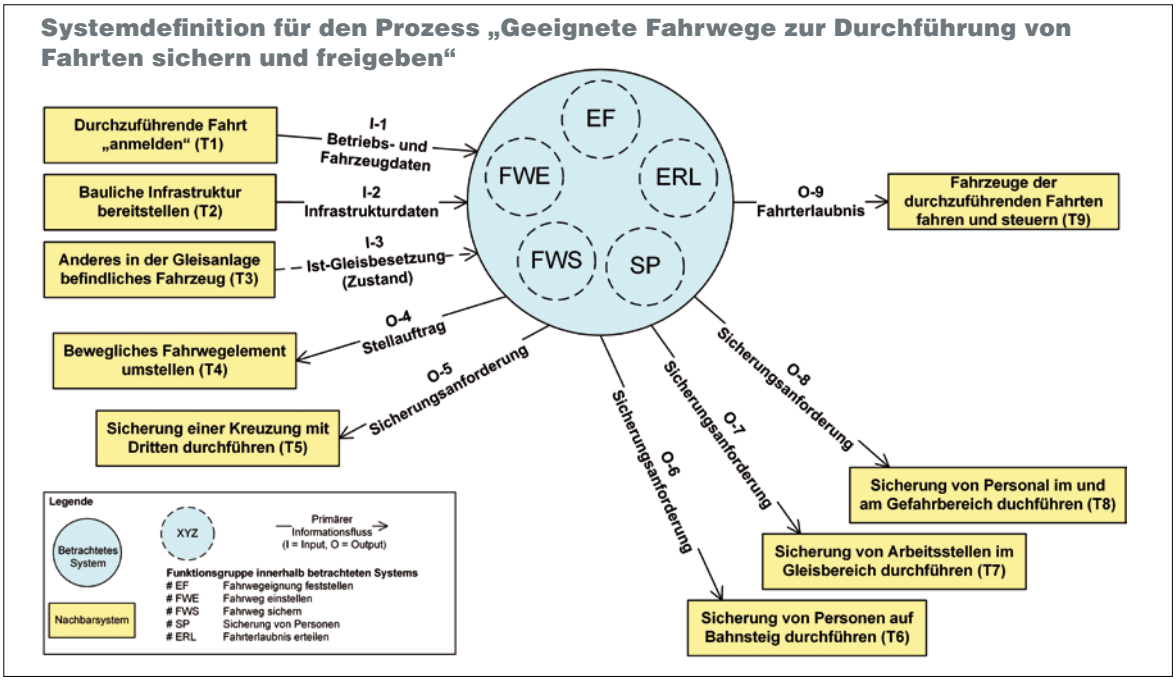
Zu den betrieblichen Randbedingungen, die im Rahmen einer Systemdefinition in der Regel zu beschreiben sind, können unter anderem Angaben zu den Geschwindigkeiten und zur Betriebsdichte gehören. Diese haben häufig Einflüsse auf mögliche Schadensausmaße und auch auf die Unfalleintrittswahrscheinlichkeiten. Zu den betrieblichen Randbedingungen können auch die örtlichen und räumlichen Umstände zählen, unter denen der Betrieb stattfindet. Als Beispiele wären hier Angaben zur Umgebung von Gleisen zu nennen, zum Beispiel, ob es sich um eine Strecke in einem Tunnel oder in offener Landschaft handelt.

Umwelt- und Einsatzbedingungen

Diese Angaben sind wichtig, um die Funktionalität des zu entwickelnden Systems auch unter den entsprechenden Bedingungen zu gewährleisten. Deshalb sind auch Angaben zum Beispiel über Kraft- und Wärmeflüsse, klimatische Verhältnisse, Erschütterungen und Vibrationen sowie elektromagnetische Beeinflussungen in eine Systemdefinition aufzunehmen.

Arbeitsweise

Selbst wenn manche Systeme auf den ersten Blick recht überschaubar wirken mögen, so ist es ratsam, Systemdefinitionen



Beispiel für eine grafische Darstellung im Rahmen einer Systemdefinition

https://doi.org/10.24355/dbbs.084-202005050944-0

nicht im stillen Kämmerlein, sondern möglichst in Arbeitsgruppen vorzunehmen. Das gemeinsame Nachdenken, Erörtern und Begründen, warum zum Beispiel etwas als Nachbarsystem betrachtet und nicht mit einbezogen werden soll, verbessern die Aussagekraft von Systemdefinitionen und sichern sie ab.

Bewährt haben sich Darstellungsformen, in denen die Elemente des zu Betrachtenden als verschiedenfarbige Kreise und Rechtecke abgebildet werden. Die Beziehungen zwischen ihnen können durch Linien und/oder Pfeile eingetragen werden (Abbildung links). Geeignete Arbeitsmittel sind Pinnwände mit farbigen Steckkarten und Flipcharts. Die so entstandenen „grafischen" Arbeitsergebnisse sollten fotografisch festgehalten und ergänzend in einem Textdokument beschrieben und erläutert werden. Stichwortartige Notizen sollten im Nachgang ausformuliert werden, um die Spielräume für nachträgliche Interpretationen einzuschränken.

Gefährdungsidentifikation

Im Teil 2 dieses Beitrags in Heft 3/2014, S. 49 ff. wurde die Gefährdung als eine Situation definiert, die vom normalen planmäßigen Betrieb eines Verkehrssystems abweicht UND aus der sich ein Unfall ergeben kann. Gefährdungen können also ermittelt werden, indem geprüft wird, ob ein unzulässiger oder nicht beabsichtigter Umstand zu einem Unfall führen kann.

Für das Identifizieren von Gefährdungen sind verschiedene Vorgehensweisen denkbar. Es kann zum Beispiel durch Brainstorming erfolgen oder auch auf der Abfrage und Auswertung von Expertenwissen beruhen. Gut bewährt haben sich systematische Methoden. Sie erlauben strukturierte und nachvollziehbare Vorgehensweisen und können deshalb dazu beitragen, die Ergebnisse im Hinblick auf die angestrebte Vollständigkeit zu verbessern.

Das Prinzip der systematischen Vorgehensweisen beruht darauf, für die zunächst im Rahmen der Systemdefinition definierten Aufgaben und Funktionen eines Systems nach einem festen Schema zu ermitteln, wie diese Funktionen versagen können und mit welchen Folgen diese Versagen einhergehen könnten. Eine bewährte und häufig angewandte Methode ist die Failure Mode and Effects Analysis (FMEA), zu Deutsch Fehlermöglichkeits- und -einflussanalyse. Sie wird im Folgenden vorgestellt.

FMEA

Die FMEA dient der Ermittlung der Versagensarten eines Systems und analysiert deren Auswirkungen. Sie ist ein Instrumentarium der vorsorgenden Fehlervermeidung und Folgenabschätzung. Die Auswirkungen eines Ausfalls im Gesamtsystem, vor allem solcher Ausfälle, die unerwünschte Auswirkungen auf den Systembetrieb haben, können ermittelt und beurteilt werden. Die FMEA ist eine wirkungsvolle Methode, mit der eine möglichst vollständige Identifizierung aller Gefährdungen unterstützt werden kann.

Die FMEA ist keine neue Methode, sondern hat in den letzten sechs Jahrzehnten sowohl in militärischen als auch diversen zivilen Feldern, wie zum Beispiel der Automobilindustrie und der Luft- und Raumfahrt, Anwendung gefunden. Eine allgemeine kontextunspezifische Normierung enthält die DIN EN 60812.

Gefährdungsidentifikation

Voraussetzung für eine möglichst umfassende Gefährdungsidentifikation ist eine lückenlose Systemdefinition. Die FMEA selbst wird in der Regel formalisiert durchgeführt, um möglichst vollständige Ergebnisse zu gewährleisten. Dabei haben sich tabellarische Vorgehensweisen bewährt.

Ausgehend von den in der Systemdefinition beschriebenen Funktionen und gegebenenfalls auch enthaltenen Systemkomponenten werden deren mögliche Fehlzustände und die daraus resultierenden Auswirkungen im System analysiert. Das Auffinden der Ausfallarten kann durch Schlüsselworte unterstützt werden. Typische Schlüsselworte zum Identifizieren der Ausfallarten enthält Tabelle 1. Sie entstammen dem Bereich elektrotechnischer Bauteile, einem der ursprünglichen Einsatzbereiche der FMEA. Sie werden in der zweiten Spalte für die Nutzung im Anwendungsgebiet interpretiert, um ein einheitliches Verständnis zu gewährleisten.

Die Abbildung auf Seite 48 zeigt am Beispiel einer Funktion „Die Solllage einer Weiche einstellen" den Aufbau einer tabellarischen FMEA. Die ersten beiden Spalten enthalten die Funktion und ihre Nummerierung. In der dritten Spalte sind die in der Tabelle 1 enthaltenen Schlüsselworte aufgeführt, mit deren Hilfe aus der Funktionsformulierung verschiedene Versagensarten abgeleitet werden. Diese werden in der vierten Spalte aufgelistet. In der Spalte „Ablauf" werden die aus dem Versagen resultierenden Abläufe beschrieben. Bei allen Abläufen, aus denen ein Unfall resultieren kann, ist das jeweilige Funktionsversagen als Gefährdung einzustufen. Kann kein Unfall eintreten, wird sich das Funktionsversagen als ein Betriebshemmnis auswirken.

In Abhängigkeit von der Art der Funktion kann in der Regel nicht bei jedem Schlüsselwort eine inhaltlich sinnvolle und nachvollziehbare Versagensformulierung gefunden werden. Die entsprechenden Zeilen bleiben leer (in der Abbildung auf S. 48 grau dargestellt).

Fallstrick „Theoretische Gefährdung"

Die Gefährdungsidentifikation ist ein rein qualitativer Prozessschritt. Die Einstufung einer Versagensart als Gefährdung geschieht vollkommen unabhängig davon, wie wahrscheinlich das Eintreten dieses Unfalls und wie groß das folgende Schadensausmaß tatsächlich sein mag. Allein die Möglichkeit eines Unfalls ist dafür ausreichend. Doch angesichts häufig sehr sicherer Systeme fällt es vielen Fachleuten schwer, ein Versagen, das aufgrund der heutigen Systeme nur sehr selten eintreten mag, als Gefährdung zu akzeptieren und in den Gefährdungskatalog aufzunehmen.

Doch sind diese Systeme nur deshalb so sicher realisiert worden, weil genau diese Gefährdung implizit vorhanden ist und mittels dieser Systeme beherrscht werden muss. Um sicherzustellen, dass nach Änderungen auch eine neue Systemrealisierung ausreichend sicher funktioniert, müssen folglich auch diese vermeintlich „theoretischen" Gefährdungen identifiziert und in den Gefährdungskatalog aufgenommen werden.

https://doi.org/10.24355/dbbs.084-202005050944-0

Eine Quantifizierung findet erst bei der Bewertung des Risikos statt. Dazu werden unter anderem die Unfalleintrittswahrscheinlichkeit und das Schadensausmaß als Bewertungsgrößen herangezogen. In diese quantifizierenden Betrachtungen fließen ferner Einflussfaktoren, wie die in der Systemsdefinition festgelegten Betriebsparameter und die Umgebungsbedingungen ein.

Risikoakzeptanzprinzipien

In dem ersten Beitrag (Deine Bahn 12/2013, S. 18 ff.) wurde bei der Einführung des Begriffs „Risiko“ festgestellt, dass „nichts zu 100 Prozent sicher ist“ und dass wir gezwungen sind, in einer Welt voller Risiken zu leben und diese ein Stück weit auch zu akzeptieren. Die vorbeugende Sicherheitsarbeit erlaubt es uns, durch systematische Vorgehensweisen den Gefährdungen eines Produktes, eines Systems bereits ins Auge zu sehen, bevor etwas passiert. Sie zwingt uns aber auch, im Vorfeld Entscheidungen zu treffen, bis zu welcher Grenze Risiken eingegangen werden dürfen, damit ein System noch als „sicher“ akzeptiert wird und als zulässig eingestuft wird.

Nach der Gefährdungsidentifikation liegt als Ergebnis eine Liste der Gefährdungen vor, die von dem betrachteten System ausgehen können. Sie müssen von der Systemrealisierung so beherrscht werden, dass von dem System keine nicht akzeptierbaren Risiken ausgehen. Für jede der ermittelten Gefährdungen muss deshalb bestimmt werden, mit welchen Maßnahmen die ausreichende Beherrschung der entsprechenden Gefährdungen gewährleistet werden soll.

Der Begriff „Risikoakzeptanzprinzipen“ steht für drei verschiedene Wege, mittels derer die Eignung der Maßnahmen zur Beherrschung der Gefährdungen nachgewiesen werden kann. Die CSM-Verordnung sieht als Risikoakzeptanzprinzipien die Anwendung der anerkannten Regeln der Technik, das Heranziehen von Referenzsystemen und das Durchführen einer expliziten Risikoabschätzung vor. Diese drei Möglichkeiten werden nachfolgend vorgestellt und erläutert.

Anerkannte Regeln der Technik

An die anerkannten Regeln der Technik stellt die CSM-Verordnung folgende Anforderungen: Sie müssen im Eisenbahnsektor allgemein anerkannt und für das System, dessen Gefährdungen betrachtet werden, relevant sein. Gegebenenfalls muss ihre Anwendung begründet und akzeptiert werden. Ferner müssen sie für alle Akteure, die sie anwenden wollen, zugänglich sein.

Das Eisenbahn-Bundesamt definiert den Begriff der anerkannten Regel der Technik in unter Bezug auf § 2 Abs. 1 EBO als „auf Erkenntnissen und Erfahrungen beruhenden geschriebenen und ungeschriebenen Regeln der Technik, deren Befolgung beachtet werden muss, um Gefahren auszuschließen, und die in den betreffenden Fachkreisen bekannt sind und als richtig anerkannt werden“. Erläuternd wird darauf hingewiesen, dass zum Beispiel auf dem Gebiet der Signal-, Telekommunikations- und elektrotechnischen Anlagen unter anderem technische Normen (EN, DIN, DIN VDE) und die Regelwerke der Eisenbahnen des Bundes als anerkannte Regeln der Technik betrachtet werden.

Kann für eine identifizierte Gefährdung gezeigt werden, dass das betrachtete System im Hinblick auf diese Gefährdung entsprechend einschlägiger Regeln und Normen entworfen, gebaut und betrieben werden kann, darf diese Gefährdung als beherrscht und das von ihr noch ausgehende verbleibende Risiko als akzeptiert gelten. Weitergehende Risikobetrachtungen sind nicht erforderlich.

Referenzsystem

Warum das Rad neu erfinden, wenn es an anderer Stelle bereits eine geeignete Lösung zu geben scheint? Dies ist der Grundgedanke, der sich hinter dem Begriff des „Referenzsystems“

Beispiel für den tabellarischen Aufbau einer FMEA

Nr.	Funktion	Schlüsselwort	Versagensart	Ablauf / Szenario	Folge	Bemerkungen/Verweise
1.1	**Solllage einer Weiche einstellen *)**	geht nicht	Die Weiche kann nicht in die Solllage gestellt werden.	Der Stellvorgang lässt sich nicht durchführen („Blockade“).	Fahrt kann nicht stattfinden → Betriebshemmnis	Bleibt die Blockade unbemerkt, liegt eine ungewollte/falsche Lage vor → s. bei „ungewollt falsch“.
		zur Unzeit (zu spät / zu früh)	Die Solllage wird zu früh eingestellt.	Die Weiche steht nicht für andere Fahrwege zur Verfügung.	Andere Fahrten werden ausgeschlossen → Betriebshemmnis	
				Eine andere Fahrt ist bereits zugelassen / findet noch statt.	Dies entspricht dem Versagen der Funktion „1.2 Solllage einer Weiche sicherstellen“, siehe dort.	
			Die Solllage wird zu spät eingestellt.	Die betrachtete Fahrt kann nicht rechtzeitig stattfinden.	Betriebshemmnis	
				Fahrt über falsche Lage oder unvollständig gestellte Weiche.	Zusammenstoß, Entgleisung → Gefährung	Maßnahme(n) erforderlich, um sicherzustellen, dass erst gefahren wird, wenn Solllage erreicht ist.
		ungewollt / falsch	Es wird eine andere Weichenlage eingestellt / erreicht.	Fahrt in ein anderes Gleis; bei Fahrt in Abzweig u.U. zu hohe Geschwindigkeit.	Zusammenstoß, Entgleisung → Gefährdung	Maßnahme(n) erforderlich, um sicherzustellen, dass die erforderliche Solllage vorliegt.
		zu niedrig / zu hoch	Sinnvolle Formulierung nicht möglich			
		zu wenig / zu viel	Die Solllage wird nur unvollständig erreicht (unvollständiger Stellweg).	Fahrt über eine nicht anliegende Weichenzunge (nicht ordnungsgemäß anliegend bzw. Mittellage).	Entgleisung → Gefährdung	Maßnahme(n) erforderlich, um sicherzustellen, dass die erforderliche Solllage ordnungsgemäß erreicht wird.
	*) Funktionsabgrenzung: Sicherstellen der eingestellten Solllage bis eine zugelassene Fahrt die Weiche verlassen hat → Funktion 1.2					

https://doi.org/10.24355/dbbs.084-202005050944-0

verbirgt. Tatsächlich ist eine solche Übernahme denkbar. Sie ist aber an eine Reihe von Voraussetzungen geknüpft, um die Angemessenheit der zu übernehmenden Lösung sicherzustellen. Dies kann der Fall sein, wenn das betrachtete System und das heranzuziehende Referenzsystem „vergleichbar" sind.

Die Vergleichbarkeit eines Referenzsystems ist auf Basis der Systemdefinition des zu betrachtenden Systems zu begründen. Dazu ist zu zeigen, dass das Referenzsystem über ähnliche Funktionen und Schnittstellen verfügt und unter ähnlichen Betriebs- und Umweltbedingungen eingesetzt wird. Ferner muss es sich bereits in der Praxis in dem Sinne bewährt haben, dass es ein akzeptables Sicherheitsniveau gewährleistet. Außerdem muss es in dem Mitgliedstaat, in dem die zu bewertende Änderung eingeführt werden soll, nach wie vor eine Genehmigung erhalten.

Explizite Risikoabschätzung

Bei den ersten beiden der drei Risikoakzeptanzprinzipien wird das Einhalten eines akzeptierten Risikos nachgewiesen, ohne dass Risikowerte ermittelt oder berechnet werden müssen. Dagegen kommen bei der expliziten Risikoabschätzung die Grundzüge der im Teil 1 vorgestellten Risikoformel zum Ansatz. Dazu werden für jede Gefährdung die Wirkungszusammenhänge zwischen der Gefährdung, den möglichen Schäden, deren Ausmaß sowie die Unfalleintrittswahrscheinlichkeiten analysiert.

Solche Analysen können qualitativ, das heißt ausschließlich beschreibend, und/oder unter Einbeziehung von Zahlen und statistischen Daten der Vergangenheit quantitativ durchgeführt werden. Ferner gibt es semiquantitative Methoden, die qualitativen Analysen zum Beispiel mit Risikoprioritätskennzahlen zu klassifizieren.

Wahl eines geeigneten Risikoakzeptanzprinzips

Die CSM-Verordnung stellt es frei, nach welchem Risikoakzeptanzprinzip das Beherrschen einer identifizierten Gefährdung nachgewiesen wird. Auch Mischformen sind denkbar. Es gilt aber in jedem Fall der Grundsatz, dass die Beherrschung der Risiken über das jeweils ausgewählte Akzeptanzprinzip methodisch korrekt und plausibel nachgewiesen werden muss. Die Basis für diesen methodischen Nachweis sind nachvollziehbare Systemdefinitionen und Gefährdungsidentifikationen.

In der Praxis wird sich die Anwendung der anerkannten Regeln der Technik als der Weg mit dem geringsten Aufwand dargestellt. Ihre Anwendung wird, wie auch schon bisher, das Standardinstrumentarium für das Nachweisen des Einhaltens eines akzeptierten Risikos bleiben. Dagegen werden explizite Risikoabschätzungen auch nach der Einführung der CSM-Verordnung nicht zum Tagesgeschäft von Eisenbahningenieuren gehören. Sie sind in der Regel nicht nur sehr aufwändig, sondern können und sollten auch nur von Experten auf dem Gebiet von Risikoanalysen und/oder in Zusammenarbeit mit ihnen durchgeführt werden. Inwieweit Referenzsysteme herangezogen werden können, wird vom Anwendungsfall abhängen. Auf den ersten Blick erscheint das System Eisenbahn als wenig vergleichbar mit anderen Verkehrssystemen. Dennoch ist es vorstellbar, dass sich für bestimmte Teilsysteme, wie zum Beispiel bei Ingenieurbauwerken oder auch bei Verfahren zur sicheren Datenübertragung Referenzen finden lassen.

Ausblick

Auch wenn Sicherheits- und Risikoanalysen im Eisenbahnwesen seit Langem ein fester Bestandteil der Sicherheitsarbeit und ein Teil der Entwicklungs- und Zulassungsprozesse neuer Systeme sind, so haben unter anderem mit der europäischen Verordnung 352/2009 „über die Festlegung einer gemeinsamen Sicherheitsmethode für die Evaluierung und Bewertung von Risiken" risikoorientierte Sichtweisen auch für die Sicherheitsnachweisführung in Bereichen an Bedeutung gewonnen, die bislang noch nicht davon betroffen schienen.

Neu eingeführte Begriffe wie Systemdefinition, Funktionsdefinition, Gefährdungsidentifikation und Risikoakzeptanz scheinen althergebrachte Vorgehensweisen, wie die Anwendung von Normen und Richtlinien, zu ersetzen. Doch bei genauerer Betrachtung sind die mit den Begriffen verbundenen Arbeitsschritte auch bei den bisherigen Vorgehensweisen zwar nicht so offensichtlich, aber letztlich implizit auch getätigt worden. Jeder Anwender einer Norm oder einer Richtlinie musste auch bisher schon darlegen, dass er sie auf den konkreten Anwendungsfall anwenden darf und warum sie geeignet ist. Auch dieses setzte bereits eine Auseinandersetzung mit dem System voraus – was im Prinzip einer impliziten Systemdefinition gleichkam. Und wer einmal hinterfragt, warum es in einer Norm oder Richtlinie eine bestimmte Regelungen oder Vorgaben gibt, wird auch auf (in der Regel nicht unmittelbar schriftlich niedergelegte) Begründungen stoßen, die dem Begriff „Gefährdung" entsprechen. Durch die sachgemäße Anwendung einer geeigneten Norm oder Richtlinie wurde sie nicht nur implizit „beherrscht", sondern auch sichergestellt, dass von dem System kein nicht akzeptierbares Risiko ausging.

Abschließend ist anzumerken, dass durch die neuen Ansätze unter Risikogesichtspunkten keine neuen Wirkungszusammenhänge geschaffen worden sind. Es wurden jedoch in der Vorgehensweise bestimmte Prozessschritte stärker akzentuiert und systematisiert, um im Sinne einer vorbeugenden Sicherheitsarbeit mögliche Sicherheitslücken besser vermeiden und Entscheidungen transparenter nachvollziehen zu können. „Alt" und „Neu" liegen möglicherweise dichter beieinander, als es den Anschein haben mag und neue Begrifflichkeiten es auch andeuten mögen. ■

Literatur

- European Railway Agency. Recommendation on the 1st set of Common Safety Methods. 12/2007
- Europäische Gemeinschaft. Verordnung (EG) Nr. 352/2009 der Kommission vom 24.04.2009 über die Festlegung einer gemeinsamen Sicherheitsmethode für die Evaluierung und Bewertung von Risiken
- DIN EN 60812. Analysetechniken für die Funktionsfähigkeit von Systemen – Verfahren für die Fehlzustandsart- und -auswirkungsanalyse (FMEA) (IEC 60812:2006), 2006
- Eisenbahn-Bundesamt. Verwaltungsvorschrift für die Bauaufsicht über Signal-, Telekommunikations- und Elektrotechnische Anlagen (VV BAU-STE), Ausgabe 4.51, Gültig ab 01.06.2010.

https://doi.org/10.24355/dbbs.084-202005050944-0